The State of Telecommuting: Privacy and Security Survey Results

Sagi Leizerov, Ph.D.

Center For Democracy & Technology

Ernst & Young

Agenda

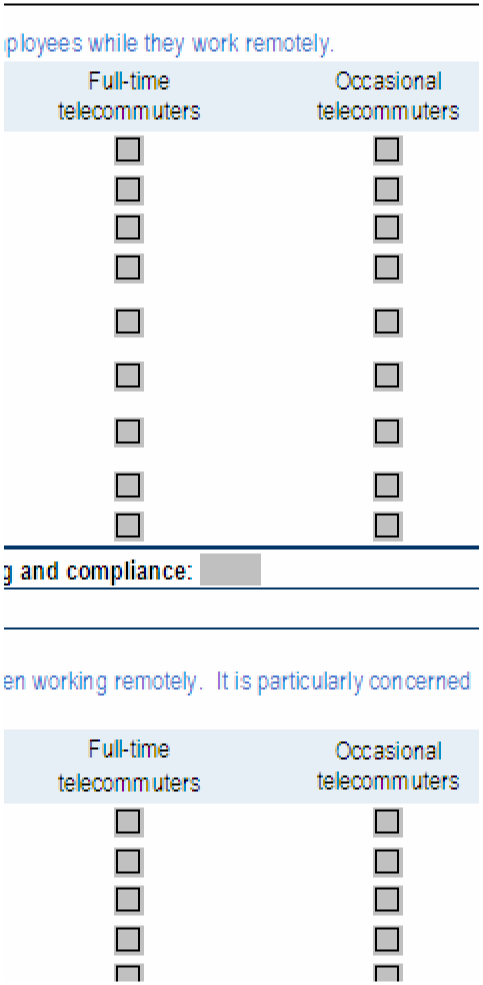
- Why telecommuting
- The survey and its respondents
- Key observations and “Practices to Adopt”

The Telecommuting Challenge

- General risks when information leaves the office
  - Loss or theft of information or devices
  - Inappropriate access by strangers
  - Communication through unprotected channels
- Risks to information in the home environment
  - Printing without appropriate disposal
  - Accessing or loading information on unprotected home devices
  - Allowing non-employees access to devices for personal use
  - Inappropriate access by non-employees residing with the telecommuter
  - Lack of privacy and security requirements
  - Lacking compliance with privacy and security requirements
- The insider threat and telecommuting
  - Purposefully extracting and inappropriately sharing information
  - Changing and manipulating hardware and software to overcome security controls

The Survey

- 15 sections, multiple questions, and text fields for questions
  - Organization Information
  - Privacy and Security Management
  - Telecommuter Employment Management
  - Temporary Employee and Contractor Employment Management
  - Computer Management
  - Installed Security Applications
  - Device Authentication and Identity Management Methods
  - Peripheral Devices
  - Internet Connectivity
  - Internal Network Access, Authentication, and Identity Management Methods
  - Accessing Applications Offline
  - Restrictions Related to Downloads, Web Sites, and Applications
  - Paper Record Management
  - Monitoring and Compliance
  - Security Considerations



ployees while they work remotely.

Full-time telecommuters	Occasional telecommuters
□	□
□	□
□	□
□	□
□	□
□	□
□	□
□	□
□	□

g and compliance:

en working remotely. It is particularly concerned

Full-time telecommuters	Occasional telecommuters
□	□
□	□
□	□
□	□
□	□

Survey Respondents

- 73 organizations in the US, Canada, and Europe
- 10 industries
- Half have Fortune designations
  - Fortune 50 (15)
  - Fortune 100 (5)
  - Fortune 500 (12)
  - Fortune 1000 (5)
- Average employees: 50,000
- Median employees: 4,000
- Ahead of the curve on governance and risk

All responding organizations have occasional telecommuters

- Nearly all employees for some
- Hard to quantify for some

46 of the 73 have full-time telecommuters

Telecommuting Guidance

Most respondents allow employees to handle personal information at home, but only half developed guidelines for telecommuting and provide guidance to their employees on the topic.

- Guidance is often not telecommuting-specific.
- In some cases, telecommuting-specific standards and training only for full-time telecommuters.
- Policies and guidance may exist but not known
- Lack of clarity over ownership of the issue.

Telecommuting Guidance

Most respondents allow employees to handle personal information at home, but only half developed guidelines for telecommuting and provide guidance to their employees on the topic.

Practices to Adopt

- Developing telecommuting-specific policies and guidance that address the organization’s specific needs and risks
- Identifying those employees who should become aware of telecommuting policies and provide them with relevant guidance

Devices Used At Home

Telecommuters commonly use their own personal computers and PDAs at home for work purposes.

- 50% of respondents’ telecommuters sometimes use their own personal computers and PDAs at home for work purposes
  - Some look to ease existing limitations regarding personal devices.
- Many organizations
  - Allow telecommuters to handle personal information at home
  - Allow/aware that telecommuters use own computers for work
  - Apply controls to organization-issued devices only.

Devices Used At Home

Telecommuters commonly use their own personal computers and PDAs at home for work purposes.

Practices to Adopt

- Prohibiting employees from using home computers without information security mechanisms installed and before clear policy and guidance are provided to them
- Providing employees with the necessary security mechanisms to be installed on home computers
- Prohibiting processing and storing the organization’s personal information on home computers

Authentication and Emerging Technologies

Few organizations have adopted thin-client terminals or biometric authentication for telecommuters.

- Only 8% of organizations issue thin clients, mainly to full-time telecommuters.
- Almost no respondents said they are using biometric technology
  - Some indicated they are considering its implementation
  - Close to 100% use username and password
  - Hard-tokens used by half of the organizations to access devices, and by 25% to access applications.
- Half of the respondents allow the handling of personal information at home, do not employ hard-drive encryption, and only require user name and password for device authentication.

Authentication and Emerging Technologies

Few organizations have adopted thin-client terminals or biometric authentication for telecommuters.

Practices to Adopt

- Utilizing hard token authentication for access to devices, networks, or applications where merited by the sensitivity of the information and according to a risk-based approach
- Start assessing the adoption of biometric technology for local authentication to high-risk devices, networks, and applications

Wireless Security

Allowing telecommuters to use wireless Internet connections is a common practice, but requiring that telecommuters use wireless security measures is less common.

- Only two-thirds of organizations that allow wireless Internet connections require some form of wireless security
  - Over half of those requiring wireless security allow use of personal devices (beware of the switch).
- Telecommuters who use easily available and unprotected wireless networks for personal use may not apply wireless security procedures when they switch to work use
  - Cisco study indicate 12% telecommuters worldwide access neighbor's connection.
- While VPN is common its of little help when information is sent to personal email accounts.

Wireless Security

Allowing telecommuters to use wireless Internet connections is a common practice, but requiring that telecommuters use wireless security measures is less common.

Practices to Adopt

- Requiring wireless security measures and providing guidance to employees on how to secure their home wireless networks
- Prohibiting telecommuters from using unprotected and unauthorized wireless networks
- Considering, where practical, disabling wireless networking features in devices provided to full-time telecommuters

Encryption

hard-drive encryption is common, but of little help when employees use their home computers for work.

- Just over half of organizations require hard-drive encryption.
  - Some encrypt all laptops and some desktops
  - Some expect employees to identify what devices require encryption
  - Some avoid hard-drive encryption all together and provide folder encryption tools.
- File and email encryption tools are common (63% and 49%)
  - Use of these tools is not affected by telecommuting (number of telecommuters or full-time/occasional ratio)
  - 70% of companies with Fortune designation have adopted these tools
  - Importance of these tools due to reliance on unsecured wireless networks.

Encryption

hard-drive encryption is common, but of little help when employees use their home computers for work.

Practices to Adopt

- Providing telecommuters with file and email encryption tools and instructing them on the proper use of the tools
- Applying encryption on all devices used by telecommuters that may contain personal information
- Using encryption to secure remote connections to the organization network

Email

Limitations on telecommuters regarding the use of email and external email services are not common.

- Less than 10% of organizations restrict external emailing of emails with or without attachments.
- About 30% of respondents prohibit telecommuters from accessing external email services, but only 20% block access to such sites.
- Close to half of respondents indicated that they encrypt their email messages; others encrypt attachments
  - Such tools are of little help if they are device-based and employees use their home computers for work.

Email

Limitations on telecommuters regarding the use of email and external email services are not common.

Practices to Adopt

- Communicating clear limitations to telecommuters on the use of personal information in email and providing them with tools to protect it
- Providing network-based email encryption solutions when allowing telecommuters to use their home computers for work
- Prohibiting processing of personal information on home computers and sending it to personal email accounts
- Monitoring what and how personal information is leaving the organization via email

Software Downloads

Limitations on downloading software and using peer-to-peer file-sharing applications are common but not prevalent.

- More than half of respondents (and all government respondents) do not permit telecommuters to download software that was not issued by the organization
  - Many have no technical controls in place to enforce these policies.
- Close to half of the organizations prohibit telecommuters from using peer-to-peer file-sharing applications and employ technical controls to prevent their use
  - A third block instant message applications
  - *75% block employee access to some sites*.

Software Downloads

Limitations on downloading software and using peer-to-peer file-sharing applications are common but not prevalent.

Practices to Adopt

- Providing clear guidance on what software may be downloaded on organization-issued devices, if any
- Prohibiting most types of file-sharing applications on organization-issued devices; if allowing telecommuters to use home computers, prohibiting the use of such applications on those devices as well
- Monitoring for compliance with communicated requirements

Monitoring Telecommuters

The higher the number of telecommuters in an organization, the more likely the organization is to monitor their use of tools and technology.

- Over 70% of organizations do some monitoring of telecommuters.
  - Visits to the homes of telecommuters are not a common practice.
  - Close to 50% review access logs to applications and databases.
  - Close to 40% monitor internal organization resources (e.g., file shares).
  - *Close to 60% monitor telecommuter email and Internet use.*
  - *Call monitoring is only common when the telecommuting employee serves in a call center capacity.*

Monitoring Telecommuters

The higher the number of telecommuters in an organization, the more likely the organization is to monitor their use of tools and technology.

Practices to Adopt

- Identifying practical and effective means to monitor the use of technology by occasional and full-time telecommuters
- Identifying practical and effective means to monitor the use of technology within organizations that only have a relatively small number of telecommuters
- Notifying employees of the fact that the organization may monitor their actions
- Conduct house visits to ensure that full-time telecommuters who handle personal information are meeting the organization requirements

Key Survey Conclusions

Telecommuting risks not effectively managed today

- Policies, tools, and controls serve broader purposes than telecommuting, leaving risk gaps
- Telecommuting-specific practices are uncommon

Call for action

- Differentiate and address telecommuting risks from ones arising in other operating environments
- Develop and communicate specific policies, tools, and controls
- Monitor the privacy and security of telecommuting arrangements

Questions?

?

Center for Democracy and Technology

Ernst & Young